

IN THE CLAIMS

Claims 1, 5, 10, and 22 are amended in this paper; claim 4 is cancelled without prejudice; and claims 25-27 are added:

1. (CURRENTLY AMENDED) An apparatus for encrypting/decrypting a real-time input stream, comprising:

a control unit receiving a data stream of bytes wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, converting the data stream into data blocks, providing the data blocks for encryption or decryption, receiving encrypted or decrypted data blocks, converting the received encrypted or decrypted data blocks into bytes, and outputting the bytes;

a key schedule unit carrying out a key schedule for every round in accordance with a variable key size so as to output a key for the encryption or decryption for each round, wherein the variable key size is one of 128, 192, and 256 bits; and

a block round unit receiving the converted data blocks from the control unit, receiving the key from the key schedule ~~unit~~ unit, encrypting or decrypting the received data blocks, and providing the encrypted or decrypted data blocks to the control unit,

wherein the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit.

2. (PREVIOUSLY PRESENTED) The apparatus of claim 1, the control unit comprising:

an input buffer storing the data stream of bytes and converting the received data stream into the data blocks having a predetermined size so as to output the converted data blocks to the block round unit; and

an output buffer receiving the data blocks encrypted or decrypted in the block round unit and converting the received data blocks into the byte units so as to output a converted data.

3. (PREVIOUSLY PRESENTED) The apparatus of claim 2, wherein the block round unit completes all round calculation of data having been currently encrypted or decrypted before a next data block is inputted from the control unit and then stores the corresponding result in the output buffer of the control unit.
4. (CANCELLED)
5. (CURRENTLY AMENDED) The apparatus of ~~claim 4~~ claim 5, the key schedule unit comprising:
 - a key expansion unit expanding the inputted key value into a size amounting to $\{\text{block size} * (\text{count of rounds} + 1)\}$; and
 - a key selection unit selecting a 128 bit key required for each round from the expanded key value so as to output the selected key to the block round unit.
6. (PREVIOUSLY PRESENTED) The apparatus of claim 1, wherein the key schedule unit expands the inputted key value into a size of $\{\text{block size} * (\text{count of rounds} + 1)\}$ and then carries out a step of selecting the 128 bit key required for each round using one key register.
7. (ORIGINAL) The apparatus of claim 6, wherein the key schedule unit comprises the key register amounting to the key value required substantially for one round.
8. (ORIGINAL) The apparatus of claim 7, wherein the key register has a capacity amounting to $\{(\text{size of an inputted block}) * (\text{size of one round})\}$.
9. (ORIGINAL) The apparatus of claim 1, wherein the control unit generates a control signal to produce the key value every round and then outputs the control signal to the key schedule unit.

10. (CURRENTLY AMENDED) An apparatus for encrypting/decrypting a real-time input data stream wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, comprising:

a control unit receiving a data stream in first data format, converting the data stream and outputting data in a second data format for encryption or decryption;

a key schedule unit in communication with the control unit and carrying out a key schedule every round in response to a variable key size and outputting a key value for the encryption or decryption for each round wherein the variable key size is one of 128, 192, and 256 bits; and

a block round unit in communication with the control unit and the key schedule unit and receiving converted data in second data format from the control unit, receiving the key from the key schedule unit so as to carry out at least one of the encryption or decryption, and outputting the encrypted or decrypted result to the control unit,

wherein the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit.

11. (PREVIOUSLY PRESENTED) The apparatus of claim 10, wherein the first data format is in bytes, and the second data format is a data block.

12. (ORIGINAL) The apparatus of claim 10, the control unit comprising:

an input buffer storing the data stream of the first data format and converting the received data stream into the data of the second data format having a predetermined size; and

an output buffer receiving data in the second data format and converting the data into the first data format.

13. (ORIGINAL) The apparatus of claim 12, wherein the block round unit substantially completes all data encryption or decryption processing before a next set of data is inputted from the control unit and stores the corresponding result in the output buffer of the control unit.
14. (PREVIOUSLY PRESENTED) The apparatus of claim 10, wherein the key schedule unit outputs a key schedule result in response to the variable key size to the block round unit in every round.
15. (ORIGINAL) The apparatus of claim 14, the key schedule unit comprising:
a key expansion unit expanding the inputted key value into a size substantially equal to $\{\text{second data format size} * (\text{count of rounds} + 1)\}$; and
a key selection unit selecting an N bit key required for each round from the expanded key value to output the selected key to the block round unit.
16. (ORIGINAL) The apparatus of claim 15, wherein the N bit key is equal to a 128 bit key.
17. (ORIGINAL) The apparatus of claim 10, wherein the key schedule unit expands the inputted key value into a size of $\{\text{second data format size} * (\text{count of rounds} + 1)\}$ and then carries out a step of selecting an N bit key for each round.
18. (ORIGINAL) The apparatus of claim 17, wherein the N bit key is equal to a 128 bit key.
19. (ORIGINAL) The apparatus of claim 15, wherein the key schedule unit has a key register capable of processing the key value required substantially for one round.
20. (ORIGINAL) The apparatus of claim 17, wherein a size of the key register is no less than $\{(\text{second data format size}) * (\text{size of one round})\}$.
21. (ORIGINAL) The apparatus of claim 10, wherein the control unit generates a control signal to produce the key value in every round.

22. (CURRENTLY AMENDED) A real-time encryption/decryption apparatus, comprising:

a control unit receiving a data stream in first data format wherein the data stream data is an MPEG data stream or a Digital Satellite Service (DSS) data stream, converting the data stream and outputting data in a second data format for encryption or decryption;

a key schedule unit in communication with the control unit and carrying out a key schedule in a predetermined period in response to a variable key size, wherein the variable key size is one of 128, 192, and ~~256-bites~~ 256 bits, and wherein the schedule unit has a key register capable of processing the key required substantially for the predetermined period; and

a block round unit in communication with the control unit and the key schedule unit and receiving converted data in second data format from the control unit, receiving the key value from the key schedule unit so as to carry out at least one of the encryption or decryption,

wherein the key schedule unit provides the key schedule to the block round unit for each round without storing expanded keys being generated by the key schedule unit.

23. (PREVIOUSLY PRESENTED) The apparatus of claim 22, wherein the first data format is in bytes, and the second data format is in a data block.

24. (PREVIOUSLY PRESENTED) The apparatus of claim 22, wherein a size of the key register is no less than $\{(\text{second data format size}) * (\text{size of one period})\}$.

25. (NEW) A method of controlling a data protection key, the method comprising:

generating a data key according to a start key signal, the data key generated according to at least one of a predetermined period and a scheduled period, wherein the scheduled period depends on a change of the data key size; checking validity of the data key; and

encrypting data corresponding to the period with the data key,
wherein the start key signal is transmitted for generating the data key.

26. (NEW) The method of claim 25, further comprising a data key valid signal provided with the data key for encryption and decryption.

27. (NEW) The method of claim 25, wherein the data are encrypted according to the start key signal in real time.